IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF TEXAS
Austin Division

INITIATE PUBLICATIONS and STEPHEN N. LISSON,	§	
Plaintiffs,	§	A03CA142JN
v.	§	Civil Action No. _____
ING GROEP N.V., a/k/a ING GROUP COMPANIES,	§	
Defendants.	§	

PLAINTIFF'S ORIGINAL COMPLAINT

TO THE HONORABLE JUDGE OF SAID COURT:

Plaintiffs bring this action for Computer Fraud, Wire Fraud, Civil Conspiracy, Racketeering, Tortious Interference, Intentional Interference with Prospective Business Advantage, Intentional Infliction of Emotional Distress, Negligent Infliction of Emotional Distress, Negligent Supervision, Misrepresentation, Common-Law Fraud, Interruption of Computer Services, Theft, Harassment, Trespass to Chattels and other attempted torts and claims seeking compensatory, punitive and special damages against Defendants jointly and severally. Counts One, Two, Three & Four are pled instanter; they will be supplemented, and the remainder will follow, in an Amended Complaint.

A. Parties

1. Plaintiffs, Initiate Publications and Stephen N. Lisson, edit and publish the website *InsiderVC.com - Insights, Data & Commentary on the Venture Capital, Private Equity and Alternative Investments Industry*, from offices in Austin, Texas.

2. Defendants, ING Groep N.V., a/k/a ING Group Companies, comprise a broad spectrum of companies owned by ING Groep N.V. (such companies referred to herein collectively as "ING"), all of whom may be served with process by serving counsel Andrew Druch, or any other authorized officer, agent or vice president, at 1325 Avenue of the Americas, 12th Floor, New York, New York 10019.

B. Jurisdiction

3. The Court has jurisdiction over this lawsuit under because the action arises under the Computer Fraud and Abuse Act (CFAA), Title 18, United States Code, § 1030. Because the CFAA provides for a federal cause of action, there is automatic federal jurisdiction.

4. The Court has supplementary jurisdiction over this lawsuit under the Wiretap Act, 18 USC § 2510-2520, Stored Communications Act, 18 USC § 2701-2710, and Racketeer Influenced And Corrupt Organizations Act (RICO), and 18 USC § 1961-1968.

C. Venue

5. Venue is proper because Defendants reside, are found, have an agent, or transacts affairs in this district.

D. Conditions Precedent

6. All conditions precedent have been performed or have occurred.

E. Background

7. Defendants' ill-deeds included using Plaintiff's website and resources in ways which constituted violations of applicable statute, law, court order, tariff, regulation, or treaty (including, but not limited to, intellectual property, communications,

privacy, criminal and international law) and in a manner intended to abuse, violate or infringe upon Plaintiff's and others' privacy or property rights.

8. Defendants' scheme to defraud Plaintiff included, but was not limited to, sending unsolicited bulk programmatic "hits" to Plaintiff's website, attempting to break or actually breaking the security of Plaintiff's computers, network and the service itself, and accessing or attempting to access accounts, messages and files which did not belong to Defendants and to which Defendants knew they had absolutely no right of access whatsoever.

9. Having thoroughly toured the publicly-viewable portions on numerous occasions and from many locations for over two years, Defendants prioritized and targeted the clearly identified *Members-Only* online Network logins because those are the gateway to copyrighted pages and Directories containing Plaintiff's intellectual property and trade secrets so coveted by Defendants. When that failed, they hacked into the server's password protection method, called ".htaccess".[1]

F. Introduction

10. The fact Defendants knew they were behaving illegally each and every time they attempted unauthorized access can easily be gleaned from the online Network login on which ING repeatedly forged and misrepresented usernames, passwords and other identification. See, for example, *Exhibit A*; as well as *Exhibit B*, the resulting security warning displayed each and every time when or if unsuccessful in logging in to the *Members-Only* area and, thereby, gaining access to all the private content located in the same protected Directories.

[1] The .htaccess file in a directory protects every file in that directory and beneath that directory from unauthorized use.

11. Yet Defendants still did not stop flooding Plaintiff with their fraudulent schemes to infiltrate, collect, and disseminate Plaintiff's confidential information. Instead, they persisted, having recognized that, on Plaintiff's server, Directories are password protected with authentication using ".htaccess" files. ".Htaccess" protected directories require logins and passwords for access. The .htaccess file resides in the protected directory, and the ".htpasswd" file contains authorized logins and passwords.

12. Worse, cynically and sneakily gambling they could overwhelm Plaintiff's security by sending a high volume of spurious data which would effectively impede -- or totally disable -- functionality of Plaintiff's system, Defendants intensified their single-minded obsession, with trespassing upon Plaintiff's intellectual property and trade secrets, by resorting to automated, programmatic means of unauthorized access and copying.

G. Facts - The ING Defendants

13. For nearly two years Defendants committed computer crimes on Plaintiff's website, *InsiderVC.com*, including repeated, harassing trespasses and deliberate, intentional, malicious attempts at unauthorized access and copying. ING can be identified from its unique domain names (ing) and Internet Protocol (IP) addresses, such as pa2.ing.nl, nyuproxy02.ing-americas.com, and 193.41.234.229.

14. ING furnished false data on Plaintiff's online network login, provided fraudulent usernames and passwords, accessed or attempted to access private areas of Plaintiff's site, forged or attempted to forge Plaintiff's name, and conducted Denial-of-Service (DoS) attacks on Plaintiff's system, fully aware their unauthorized use of Plaintiff's own and others users' accounts constituted a breach or attempted breach of

security on Plaintiff's web site. Finally, Plaintiff requested, in writing, that they cease & desist.

15. Defendants assured Plaintiff, in writing, that their complained-of behavior would stop then and there. But Defendants did not in fact stop there, at manual attempts to breach security and gain access to Plaintiff's private information through fraudulent means. ING then resorted to multiplying and automating DoS attacks. Contrary to their own written assurances, Defendants soon thereafter returned to Plaintiff's site yet again, this timed armed with a nasty, virulent software program.

16. Employing this infectious, destructive software program and pointing it both at Plaintiff's password-protected Directories and hidden system files (including .htaccess and .htpasswd), Defendants maliciously generated and unleashed over 2,385 attempts to hack/crack into root access to Plaintiff's computer servers[2], password files, and other such protected content and data. Specific examples include those on September 30, 2002, at 9:22:20 a.m. CDST, and again at 9:22:22 a.m. CDST, when Defendants cracked the server's .htaccess file.

17. Defendants successfully hacked into not only the .htaccesss file but also the ".htpasswd" file. The ".htpasswd" file contains the user name and password combinations to allow login into the admin (administrative) area. The code inside the .htpasswd file containing the username and encrypted password combinations is in case-sensitive format; the latter a requirement for the login to complete. Defendants had by then realized that even if they gambled on correctly guessing a username and password combination, for it to work they needed to enter each character in the proper case-

[2] With "root access", Defendants could replace Plaintiff's login with their own, or input the Unix command "rm-rf/" to delete all files on the server, including all operating system software.

sensitive format. Hence their priority on targeting encrypted data in Plaintiff's .htpasswd file.

H. Facts - ING's Co-Defendants

18. ING committed these crimes over various Internet backbones, systems and networks, including their own, in violation of those internal or external providers' (ISP's) and system operators' (Sysops') acceptable use policies, which are designed to help protect the ISP, the ISP's customers and the Internet community in general from irresponsible or, in this case, illegal activities. Defendants, their Sysops and providers monitored, coordinated, processed, sent, relayed, routed, processed, compiled, allowed, assembled and executed the applications and actions causing these activities.

19. Actions prohibited include the very activities committed by ING. For example: "Unauthorized attempts by a user to gain access to any account or computer resource not belonging to that user (e.g., "cracking") . . . Knowingly engage in any activities that will cause a denial-of-service (e.g., synchronized number sequence attacks) to any [ISP] customers or end-users whether on the [ISP] network or on another provider's network."

20. Other "illegal activities" purportedly prohibited yet nonetheless facilitated in this case: "Advertising, transmitting, or otherwise making available any software, program, product, or service that is designed to violate [the Policy] or the [Policy] of any other Internet Service Provider, which includes, but is not limited to, the facilitation of the means to send e-mail spam, initiation of pinging, flooding, mail-bombing, denial of service attacks, and piracy of software."

21. Defendants had the right, responsibility and ability both to control their

behavior and reap direct financial benefit from it. Defendants' active monitoring of their internal and external systems and networks, and the notice they received from Plaintiff, gave them actual or putative knowledge of their users' conduct and content, and the liabilities they faced for the actions of their users (both internal and external). These are "strict liability torts," meaning that intent to violate is not a prerequisite.

I. Count One - Computer Fraud

22. Plaintiff incorporates herein by reference Paragraphs 1 through 21.

23. The CFAA provides for a civil action to help anyone injured by the criminal activity this statute prohibits. Protection covers all computers involved in interstate and foreign commerce.

24. Defendants' malicious "cracking" (unauthorized attempts to gain access to accounts and computer resources not belonging to them), knowingly engaging in activities that caused DoS attacks, furnishing false data on Plaintiff's online network login, and providing fraudulent usernames and passwords, constituted a breach or attempted breach of security on Plaintiff's site.

25. Thus, Plaintiff has causes of action against Defendants for fraud, as expressed in 18 USC § 1030(a)(4).

J. Count Two - Interruption of Computer Services

26. Plaintiff incorporates herein by reference Paragraphs 1 through 21.

27. It is a crime also to interrupt computer services either to the provider of those computer services or the users of that system. Defendants' ill-deeds degraded access both to Plaintiff's services and system.

28. Defendants' excessive use of Plaintiff's property and resources limited

and interfered with the bandwidth available to others through such fraudulent means as an automated software program whose sole intent is creating a continuous connection and hijacking Plaintiff's website, and "bombing" (multiple messages sent to specific destinations on Plaintiff's site with the intent to render it inoperable or dysfunctional).

29. Defendants' knew that by perpetrating these dishonest methods and schemes, Plaintiff would be forced to withhold or delay the use of computer services by or to legitimate subscribers.

30. Thus, Plaintiff has a cause of action against Defendants for interruption of computer services, over Defendants' disruption to Plaintiff's system.

K. Count Three - Wire Fraud

31. Plaintiff incorporates herein by reference Paragraphs 1 through 21.

32. 18 USC § 1343 makes it a Federal crime or offense for anyone to use interstate wire communications facilities in carrying out a scheme to defraud.

33. In Defendants' knowingly and willfully devising or intending to devise a scheme to defraud, the use of the interstate wire communications facilities was closely related to the scheme because Defendants either wired something or caused it to be wired in interstate commerce in an attempt to execute or carry out the scheme.

34. Defendants' deliberate scheme to defraud by and through gaining unauthorized access (it matters not whether successful) included but was not limited to repeatedly, forging and misrepresenting usernames, passwords and other identification; adding or attempting to add member logins without Plaintiff's explicit positive consent; attempting to cancel, supersede, or otherwise interfere with e-mail or content posted on or through Plaintiff's site; harassment through frequency and size of both manual and

automated attempts to hack/crack and programmatic "hits"; engaging in synchronous flood attacks (overburdening a recipient computer system by sending a high volume of spurious data which effectively impedes or totally disables functionality of the recipient system).

35. Each separate use of the interstate wire facilities in furtherance of Defendants' scheme to defraud constitutes a separate offense; in this case, over 2,000.

L. Count Four - Racketeering

36. Plaintiff incorporates herein by reference Paragraphs 1 through 21.

37. Civil RICO (Section 1964(c)) permits "'[a]ny person injured in his business or property by reason of a violation' of RICO's criminal provisions to recover treble damages and attorney's fees."

38. All the elements to prove RICO violations against Defendants exist here: Plaintiff was injured by a person associated with an "enterprise" that has been engaging in a "pattern of racketeering," which consists of at least two "predicate acts" during a ten-year period.

39. The list of "predicate acts" includes wire fraud.

M. Damages

40. Defendants incurred criminal and civil liability for violating Plaintiff's system and network security, including unauthorized access to or use of Plaintiff's data, systems and networks, attempts to probe, scan or test the vulnerability of Plaintiff's system and network and to breach security or authentication measures without Plaintiff's express authorization.

41. The CFAA makes it clear that civil damages are a recognized form of

relief. Section 1030(g) of the Act states, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Defendants' offenses caused losses aggregating at least $5,000 in value over the course of one year.

42. As the proximate result of the aforementioned acts, including their unauthorized monitoring of data or traffic on Plaintiff's network and system without express authorization, their interference (mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks) with service to any user, host or network, Plaintiffs suffered losses and damages exceeding the jurisdictional minimum of the statute.

43. Plaintiff's damages under 18 U.S.C. §1030 (e)(8) include impairment to the integrity and availability of its computer data, systems, information, and services that caused a loss of at least $5,000. An impairment of the data's integrity may occur even though no data was physically changed or erased if the victim suffered a "loss". Impairment can include the alleged access and disclosure of trade secrets when the data was copied rather than modified.

44. "Loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, programs, systems, information and services to their condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service or the interference with service to any user, host, or network.

45. Plaintiff's losses include monetary loss sustained as a result of damage to

its computer data, systems, information, and services. The calculation of damages is based not only on the resulting impairment, but also includes the cost in time and resources, plus all measures to restore and secure the data, systems, information, and services. The damage and thus violation to integrity was caused by the alleged infiltration and the collection and dissemination of confidential information.

46. Defendants "cracking" and "hacking" of any host, network, or account circumvented Plaintiff's user authentication and security. As the target, fearing that the actual damage might scare customers and have an adverse affect on business, Plaintiff is incentivized to minimize losses. Fortunately, claims may be made under the CFAA even if an unauthorized intrusion does not in and of itself cause any damage to the computer system in question.

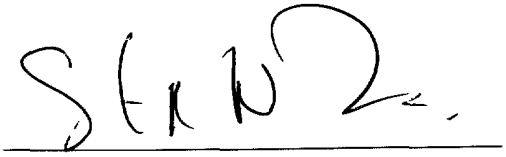
47. Additionally, each and every single one of Defendants' thousands of attempted offenses if completed would have caused losses aggregating at least $5,000 in value over the course of one year.

N. Prayer

FOR THESE REASONS, Plaintiff asks for judgment against Defendants, actual exemplary, special, punitive and treble damages, prejudgment and postjudgment interest, costs of suit, plus all other relief the court deems appropriate.

Respectfully submitted,

INITIATE PUBLICATIONS and
STEPHEN N. LISSON, Pro Se



Stephen N. Lisson
Post Office Box 2013

Austin, TX 78768-2013
Tel. (512) 473-7110
Fax (512) 473-7120

STATE OF TEXAS §
COUNTY OF TRAVIS §

AFFIDAVIT OF STEPHEN N. LISSON

On this day, Stephen N. Lisson appeared before me, the undersigned notary public. After I administered an oath to him, upon his oath, he said:

"My name is Stephen N. Lisson. I am competent to make this affidavit. The fact stated in Plaintiff's Original Complaint are within my personal knowledge and are true and correct."

Stephen N. Lisson

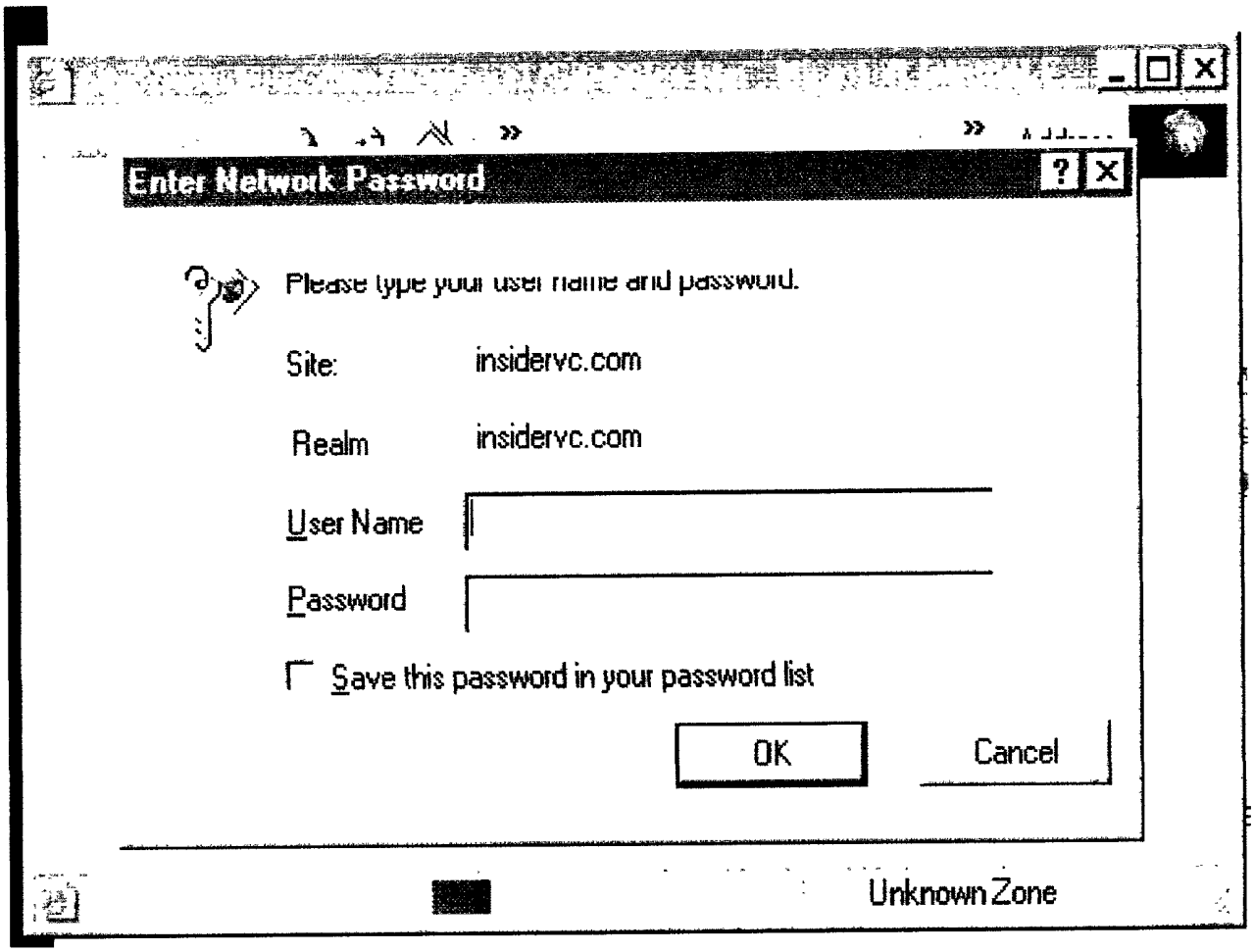
SWORN TO and SUBSCRIBED before me by Stephen N. Lisson on March 07, 2003.

JAMES MIRE
NOTARY PUBLIC STATE OF TEXAS
COMMISSION EXPIRES:
DECEMBER 17, 2006

Notary Public in and for
The State of Texas
Travis County

EXHIBIT

A


Enter Network Password
Please type your user name and password.
Site: insidervc.com
Realm insidervc.com
User Name
Password
Save this password in your password list
OK
Cancel
Unknown Zone

EXHIBIT

B

You are not authorized to view this page

You do not have permission to view this directory or page using the credentials you supplied.

Please try the following:

- Click the Refresh button to try again with different credentials.
- If you believe you should be able to view this directory or page, please contact the Web site administrator by using the e-mail address or phone number listed on the home page.

HTTP 401.3 - Access denied by ACL on resource
Internet Information Services

Technical Information (for support personnel)

- More information:
  Microsoft Support